Computer Network Attack: What it is, warning signs, and how to defend fast

Gridinsoft Help Center

What it is

A computer network attack is a deliberate hit on your systems to break, slow, or quietly take control. Attackers exploit weak spots in apps, devices, or configurations to spread malware, steal data, or flood services with traffic (DDoS) until they stall.

How it plays out

- Break-in: phishing, stolen passwords, or unpatched bugs.
- Action: plant malware, move sideways, or launch a DDoS to knock services offline.
- Impact: outages, data theft, ransom demands, or hijacked accounts.

Signs to watch for

- Sudden slowdowns or outages; login spikes or lockouts
- New admin tasks/services; security tools disabled
- Unusual data transfers or repeated connections to unknown hosts

Defend smart

- Patch fast (VPNs, email, web apps) and remove unused remote access.
- MFA everywhere and least-privilege admin rights.
- EDR/AV + DNS filtering to catch malware and beaconing.
- Rate limits/WAF & DDoS protection at the edge.
- Backups and runbooks-practice restore drills.

If you’re under attack (first steps)

- Isolate affected hosts or services.
- Block malicious IPs/domains; enable rate limits.
- Collect logs/evidence before wiping or rebooting.
- Rotate credentials from a clean device; check access tokens/keys.
- Restore from known-good backups; review what to harden.